The RSA scheme capitalizes on the relative ease of creating a composite number from the product of two prime numbers whereas the attempt to factor the composite number into its constituent primes is difficult. The RSA scheme uses a public key E comprising a pair of positive integers n and e, where n is a composite number of the form

$$n=p\cdot q \quad (1)$$

where p and q are different prime numbers, and e is a number relatively prime to (p-1) and (q-1); that is, e is relatively prime to (p-1) or (q-1) if e has no factors in common with either of them. Importantly, the sender has access to n and e, but not to p and q. The message M is a number representative of a message to be transmitted wherein

$$0\leq M\leq n-1. \quad (2)$$

The sender enciphers M to create ciphertext C by computing the exponential

$$[C=M^e(\text{mod } n)]\ \underline{C\equiv M^e(\text{mod } n)}. \quad (3)$$

Replace the paragraph beginning at col. 2, line 19 with the following:

The recipient of the ciphertext C retrieves the message M using a (private) decoding key D, comprising a pair of positive integers d and n, employing the relation

$$[M=C^d\ (\text{mod } n)]\ \underline{M\equiv C^d(\text{mod } n)} \quad (4)$$

As used in (4), above, d is a multiplicative inverse of

$$e(\text{mod}(\text{lcm}((p-1), (q-1)))) \quad (5)$$

so that

$$[e\cdot d=1(\text{mod}(\text{lcm}((p-1), (q-1))))]\ \underline{e\cdot d\equiv 1(\text{mod}(\text{lcm}((p-1), (q-1))))} \quad (6)$$

where lcm((p-1), (q-1)) is the least common multiple of numbers p-1 and q-1. Most commercial implementations of RSA employ a different, although equivalent, relationship for obtaining d:

$$[d=e^{-1}\ \text{mod}(p-1)\ (q-1)]\ \underline{d\equiv e^{-1}\ \text{mod}((p-1)\cdot(q-1))}. \quad (7)$$

This alternate relationship simplifies computer processing.

Replace the paragraph beginning at col. 3, line 23 with the following:

It is still another object of this invention to provide a system and method for implementing an RSA scheme in which the [components] <u>factors</u> of n do not increase in length as n increases in length.

Replace the paragraph beginning at col. 3, line 27 with the following:

It is still another object to provide a system and method for utilizing multiple (more than two), distinct prime number [components] factors to create n.

Replace the paragraph beginning at col. 3, line 36 with the following:

The present invention discloses a method and apparatus for increasing the computational speed of RSA and related public key schemes by focusing on a neglected area of computation inefficiency. Instead of $n=p \cdot q$, as is universal in the prior art, the present invention discloses a method and apparatus wherein n is developed from three or more distinct random prime numbers; i.e., $n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where k is an integer greater than 2 and p_1, p_2,. . . p_k are sufficiently large distinct random primes. Preferably, "sufficiently large primes" are prime numbers that are numbers approximately 150 digits long or larger. The advantages of the invention over the prior art should be immediately apparent to those skilled in this art. If, as in the prior art, p and q are each on the order of, say, 150 digits long, then n will be on the order of 300 digits long. However, three primes p_1, p_2 and p_3 employed in accordance with the present invention can each be on the order of 100 digits long and still result in n being 300 digits long. Finding and verifying 3 distinct primes, each 100 digits long, requires significantly fewer computational cycles than finding and verifying 2 primes each 150 digits long.

Replace the paragraph beginning at col. 3, line 56 with the following:

The commercial need for longer and longer primes shows no evidence of slowing; already there are projected requirements for n of about 600 digits long to forestall incremental improvements in factoring techniques and the ever faster computers available to break ciphertext. The invention, allowing 4 primes each about 150 digits long to obtain a 600 digit n, instead of two primes about [350] 300 digits long, results in a marked improvement in computer performance. For, not only are primes that are 150 digits in size easier to find and verify than ones on the order of [350] 300 digits, but by applying techniques the inventors derive from the Chinese Remainder Theorem (CRT), public key cryptography calculations for encryption and decryption are completed much faster--even if performed serially on a single processor system. However, the inventors' techniques are

particularly adapted to [be] advantageously apply [enable] RSA public key cryptographic operations to parallel computer processing.

Replace the paragraph beginning at col. 4, line 6 with the following:

The present invention is capable of [using] extending the RSA scheme to perform encryption and decryption operation using a large (many digit) n much faster than heretofore possible. Other advantages of the invention include its employment for decryption without the need to revise the RSA public key encryption transformation scheme currently in use on thousands of large and small computers.

Replace the paragraph beginning at col. 4, line 13 with the following:

A key assumption of the present invention is that n, composed of 3 or more sufficiently large distinct prime numbers, is no easier (or not very much easier) to factor than the prior art, two prime number n. The assumption is based on the observation that there is no indication in the prior art literature that it is "easy" to factor a product consisting of more than two sufficiently large, distinct prime numbers. This assumption may be justified given the continued effort (and failure) among experts to find a way "easily" to break large [component] composite numbers into their large prime factors. This assumption is similar, in the inventors' view, to the assumption underlying the entire field of public key cryptography that factoring composite numbers made up of two distinct primes is not "easy." That is, the entire field of public key cryptography is based not on mathematical proof, but on the assumption that the empirical evidence of failed sustained efforts to find a way systematically to solve NP problems in polynomial time indicates that these problems truly are "difficult."

Replace the paragraph beginning at col. 4, line 32 with the following:

The invention is preferably implemented in a system that employs parallel operations to perform the encryption, decryption operations required by the RSA scheme. Thus, there is also disclosed a cryptosystem that includes a central processor unit (CPU) coupled to a number of exponentiator elements. The exponentiator elements are special

purpose arithmetic units designed and structured to be provided message data M, an encryption key e, and a number n (where [$n=p_1 * p_2 * \ldots p_k$] $\underline{n= p_1 \cdot p_2 \cdot \ldots \cdot p_k}$, k being greater than 2) and return ciphertext C according to the relationship,

[$C=M^e \pmod{n}$] $\underline{C \equiv M^e \pmod{n}}$.

Replace the paragraph beginning at col. 4, line 45 with the following:

Alternatively, the exponentiator elements may be provided the ciphertext C, a decryption (private) key d and n to return M according to the relationship,

[$M=C^d \pmod{n}$] $\underline{M \equiv C^d \pmod{n}}$

Replace the paragraph beginning at col. 4, line 50 with the following:

According to this decryption aspect of the invention, the CPU receives a task, such as the requirement to decrypt [cyphertext] ciphertext data C. The CPU will also be provided, or have available, a [public] private key [e] d and n, and the factors of n (p_1, p_2, . . . p_k). The CPU breaks the [encryption] decryption task down into a number of sub-tasks, and delivers the sub-tasks to the exponentiator elements. [When the] The results of the sub-tasks are returned by the exponentiator elements to the CPU which [will], using a form of the CRT, combines the results to obtain the message data M. An encryption task may be performed essentially in the same manner by the CPU and its use of the exponentiator elements. However, usually the factors of n are not available to the sender (encryptor), only the public key, e and n, so that no sub-tasks are created.

*Before the paragraph beginning at col. 5, line 52, **insert** the following paragraph:*

Alternatively, a message data M can be encoded with the private key to a signed message data M_s using a relationship of the form

$$M_s \equiv M^d \pmod{n}.$$

The message data M can be reproduce from the signed message data M_S by decoding the signed data with the public key, using a relationship of the form

$$M \equiv M_s^e \pmod{n}.$$

Replace the paragraph beginning at col. 5, line 30 with the following:

According to the present invention, the public key portion e is picked. Then, three or more random large, distinct prime numbers, $p_1, p_2, \ldots, p_k$ are developed and checked to ensure that each (p_i-1) is relatively prime to e. Preferably, the prime numbers are of equal length. Then, the product $[n=p_1, p_2, \ldots, p_k]$ $n= p_1 \cdot p_2 \cdot \ldots p_k$ is computed.

Replace the paragraph beginning at col. 5, line 36 with the following:

Finally, the decryption [key] exponent, d, is established by the relationship:

$[d=e^{-1} \bmod ((p_1 -1)(p_2 -1) \ldots (p_k -1))]$ $d\equiv e^{-1} \bmod ((p_1 -1)\cdot(p_2 -1)\cdot \ldots \cdot(p_k - 1))$, or equivalently

$$d\equiv e^{-1} \bmod (\mathrm{lcm}((p_1 -1), (p_2 -1), \ldots (p_k -1)))$$

Replace the paragraph beginning at col. 5, line 41 with the following:

The message data, M is encrypted to ciphertext C using the relationship of (3), above, i.e.,

$[C=M^e \bmod n.]$ $C\equiv M^e \pmod n$

Replace the paragraph beginning at col. 5, line 46 with the following:

To decrypt the ciphertext, C, the relationship of [(3)] (4), above, is used:

$[M=C^d \bmod n]$ $M\equiv C^d \pmod n$

where n and d are those values identified above.

Replace the paragraph beginning at col. 5, line 52 with the following:

Using the present invention involving three primes to develop the product n, RSA encryption and decryption time can be substantially less than an RSA scheme using two primes by dividing the encryption or decryption task into sub-tasks, one sub-task for each distinct prime. (However, breaking the encryption or decryption into subtasks requires knowledge of the factors of n. This knowledge is not usually available to anyone except the owner of the key, so the encryption process can be accelerated only in special cases, such as encryption for local storage. A system encrypting data for another user performs the encryption process according to (3), independent of the number of factors of n. Decryption, on the other hand, is performed by the owner of a key, so the factors of n are generally known and can be used to accelerate the process.) For example, assume that

three distinct primes, p_1, p_2, and p_3, are used to develop the product n. Thus, decryption of the ciphertext, C, using the relationship

$$[M=C^d \pmod n] \; M \equiv C^d \pmod n$$

is used to develop the decryption sub-tasks:

$$[M_1 = C_1^{d_1} \bmod p_1] \; M_1 \equiv C_1^{d_1} \pmod{p_1}$$

$$[M_2 = C_2^{d_2} \bmod p_2] \; M_2 \equiv C_2^{d_2} \pmod{p_2}$$

$$[M_3 = C_3^{d_3} \bmod p_3] \; M_3 \equiv C_3^{d_3} \pmod{p_3}$$

where

$$[C_1 = C \bmod p_1;] \; C_1 \equiv C \pmod{p_1};$$

$$[C_2 = C \bmod p_2;] \; C_2 \equiv C \pmod{p_2};$$

$$[C_3 = C \bmod p_3;] \; C_3 \equiv C \pmod{p_3};$$

$$[d_1 = d \bmod (p_1 - 1)] \; d_1 \equiv d \pmod{(p_1 - 1)};$$

$$[d_2 = d \bmod (p_2 - 1)] \; d_2 \equiv d \pmod{(p_2 - 1)}; \text{ and}$$

$$[d_3 = d \bmod (p_3 - 1)] \; d_3 \equiv d \pmod{(p_3 - 1)}.$$

Replace the paragraph beginning at col. 6, line 24 with the following:

The results of each sub-task, M_1, M_2, and M_3 can be combined to produce the plaintext, M, by a number of techniques. However, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme. Generally, the plaintext M is obtained from the combination of the individual sub-tasks by the following relationship:

$$Y_i \equiv Y_{i-1} + ((M_i - Y_{i-1})\,(w_i^{-1} \pmod{p_i}) \pmod{p_i}) \cdot w_i \pmod n \; [Y_i = Y_{i-1} + [(M_i - Y_{i-1})\,(w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n]$$

where $[i \geq 2]$ $2 \leq i \leq k$ where k is the number of prime factors of n, and

$$M = Y_k,\; Y_1 = C_1,\; \text{and } w_i = \prod_{j<i} p_j$$

Encryption is performed in much the same manner as that used to obtain the plaintext M, provided (as noted above) the factors of n are available. Thus, the relationship

$$[C=M^e \pmod n] \; C \equiv M^e \pmod n,$$

can be broken down into the three sub-tasks,

$[C_1 = M_1^{e1} \bmod p_1]$ $C_1 = M_1^{e_1} (\bmod p_1)$,

$[C_2 = M_2^{e2} \bmod p_2]$ $C_2 = M_2^{e_2} (\bmod p_2)$ and

$[C_3 = M_3^{e3} \bmod p_3]$ $C_3 = M_3^{e_3} (\bmod p_3)$,

where

$[M_1 = M(\bmod p_1)]$ $M_1 \equiv M (\bmod p_1)$,

$[M_2 = M(\bmod p_2)]$ $M_2 \equiv M (\bmod p_2)$,

$[M_3 = M(\bmod p_3)]$ $M_3 \equiv M (\bmod p_3)$,

$[e_1 = e \bmod (p_1 - 1)]$ $e_1 \equiv e \bmod (p_1 - 1)$,

$[e_2 = e \bmod (p_2 - 1)]$ $e_2 \equiv e \bmod (p_2 - 1)$, and

$[e_3 = e \bmod (p_3 - 1)]$ $e_3 \equiv e \bmod (p_3 - 1)$.

Replace the paragraph beginning at col. 6, line 65 with the following:

In generalized form, the ciphertext C (i.e., [decrypted] encrypted message M) can be obtained by [the same summation] a recursive scheme as identified above to obtain the ciphertext C from its contiguous constituent sub-tasks C_i.

Replace the paragraph beginning at col. 7, line 1 with the following:

Preferably, the recursive CRT method described above is used to obtain either the ciphertext[,] C[,] or the deciphered plaintext (message) M due to its speed. However, there may be [occasions] implementations when it is beneficial to use a non-recursive technique in which case the following relationships are used:

$$M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} (\bmod p_i)) \cdot w_i (\bmod n) \quad [M = \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i)\, w_i \bmod n]$$

where

$$[w_i = \prod_{j \neq 1} p_j] \; w_i = \prod_{j \neq i} p_j, \text{ and}$$

k is the number (3 or more) of distinct primes chosen to develop the product n.

Replace the paragraph beginning at col. 7, line 17 with the following:

Thus, for example above (k=3), M is constructed from the returned sub-task values M_1, M_2, M_3 by the relationship

$$[M=M_1 (w_1^{-1} \bmod p_1)\, w_1 \bmod n + M_2 (w_2^{-1} \bmod p_2)\, w_2 \bmod n +$$
$$M_3 (w_3^{-1} \bmod p_3)\, w_3 \bmod n] \quad \underline{M \equiv M_1 (w_1^{-1} (\bmod p_1))\cdot w_1 (\bmod n)}$$
$$\underline{+ M_2 (w_2^{-1} (\bmod p_2))\cdot w_2 (\bmod n)}$$
$$\underline{+ M_3 (w_3^{-1} (\bmod p_3))\cdot w_3 (\bmod n)}$$

where

$$w_1 = p_2 p_3,\ w_2 = p_1 p_3, \text{ and } w_3 = p_1 p_2.$$

Replace the paragraph beginning at col. 7, line 52 with the following:

The I/O bus 30 communicatively connects the CPU to a number of exponentiator elements [32_a, 32_b, and 32_c]32a, 32b and 32c. Shown here are three exponentiator elements, although as illustrated by the "other" exponentiators [32_n]32n, additional exponentiator elements can be added. Each exponentiator element is a state machine controlled arithmetic circuit structured specifically to implement the relationship described above. Thus, for example, the exponentiator 32a would be provided the values M_1, e_1, and p_1[, n] to develop C_1. Similarly, the exponentiator circuits 32b and 32c develop C_2 and C_3 from corresponding subtask values M_2, e_2, [P_2]p_2, M_3, e_3, and [P_3]p_3.

Replace the paragraph beginning at col. 8, line 1 with the following:

In order to ensure a secure environment, it is preferable that the cryptosystem 10 meet the Federal Information [Protection System] Processing Standard (FIPS) 140-1 level 3. Accordingly, the elements that make up the CPU 14 would be implemented in a design that will be secure from external probing of the circuit. However, information communicated on the I/O bus 30 between the CPU 14 and the exponentiator circuits 32 (and external memory 34--if present) is exposed. Consequently, to maintain the security of that information, it is first encrypted by the DES unit 24 before it is placed on the I/O bus 30 by the CPU 14. The exponentiator circuits 32, as well as the external memory 34, will also include similar DES units to decrypt information received from the CPU, and later to encrypt information returned to the CPU 14.

Replace the paragraph beginning at col. 8, line 62 with the following:

In similar fashion, information is conveyed to or retrieved from the exponentiators 32 by the processor 20 by write or read operations at addresses within the address range 44. Consequently, writes to the exponentiators 32 will use the DES unit 24 to encrypt the information. When that (encrypted) information is received by the exponentiators 32, it is decrypted by on-board DES units (of each exponentiator 32). The result[s] of the task performed by the exponentiator 32 is then encrypted by the exponentiator's on-board DES unit, retrieved by the processor 20 in encrypted form and then decrypted by the DES unit 24.

Replace the paragraph beginning at col. 9, line 24 with the following:

Assume, for the purpose of the remainder of this discussion, that the encryption/decryption tasks performed by the cryptosystem 10, using the present invention, employs only three distinct primes, p_1, p_2, p_3. The processor 20 will develop the sub tasks identified above, using M, e, p_1 p_2, p_3. Thus, for example, if the exponentiator 32a were assigned the sub-task of developing C_1, the processor would develop the values M_1[,] and e_1[, and (p_1 -1)] and deliver [units] (write) these values, with [n]p_1, to the exponentiator 32a. Similar values will be developed by the processor 20 for the sub-tasks that will be delivered to the exponentiators 32b and 32c.

Replace the paragraph beginning at col. 10, line 15 with the following:

Alternatively, the [post]host-system 50 may desire to deliver, via the communication medium 60, an encrypted communication to one of the stations 64. If the communication is to be encrypted by the DES scheme, with the DES key encrypted by the RSA scheme, the host system would encrypt the communication, forward the DES key to one of the cryptosystems 10 for encryption via the RSA scheme. When the encrypted DES key is received back from the cryptosystem 10, the host system can then deliver to one or more of the stations 64 the encrypted message.

Replace the paragraph beginning at col. 10, line 25 with the following:

Of course, the host system 50 and the stations 64 will be using the RSA scheme of public key encryption/decryption. Encrypted communications from the stations 64 to the host system 50 require that the stations 64 have access to the public key [E (E, N)] E=(e, n) while the host system maintains the private key [D (D, N,] D=(d, n) and the constituent primes, $p_1, p_2, \ldots, p_k$). Conversely, for secure communication from the host system 50 to one or more of the stations 64, the host system would retain a public key E' for each station 64, while the stations retain the corresponding private keys [E'] D'.

Replace the paragraph beginning at col. 10, line 35 with the following:

Other techniques for encrypting the communication could used. For example, the communication could be entirely encrypted by the RSA scheme. If, however, the message to be communicated[ion] is represented by a numerical value greater than n-1, it will need to be broken up into blocks size M where

$[0 \leq M \leq N-1]$ $0 \leq M \leq n-1$.

In the Claims

Without prejudice or surrender of any subject matter, cancel claim 8, amend claims 1-7 and 9-13 (following the format of the claims as presented herein, including insertion of new lines and indentations where applicable), and add new claims 14-61, all of the changes to be made vis-à-vis the U.S. Patent 5,848,159, as follows:

1. (Twice Amended) A method for [establishing cryptographic] communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:

developing k distinct random prime numbers $p_1, p_2, \ldots p_k$, where k is an integer greater than 2;

providing a number e relatively prime to $(p_1 -1)\cdot(p_2 -1)\cdot\ldots\cdot(p_k-1)$;

providing a composite number n equaling the product $p_1\cdot p_2\cdot\ldots\cdot p_k$;

receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of [a] the message and

$0 \leq M \leq n-1$,

[n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2, p_1, p_2, . . . p_k are distinct prime numbers, and] where C is a number representative of an encoded form of the plaintext message word signal M such that

$C \equiv M^e \pmod{n}$, and where e is associated with an intended recipient of the ciphertext word signal C; and [, wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$C=M^e \pmod{n}$

where e is a number relatively prime to $(p_1 -1)\cdot(p_2 -1)$]

deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime numbers $p_1, p_2, \ldots p_k$.

2. (Twice Amended) The method according to claim 1, [comprising the further step of:] wherein the deciphering step includes

establishing a number, d, as a multiplicative inverse of

$e(\text{mod}(\text{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$, and

decoding the ciphertext word signal C to the plaintext message word signal M[, wherein said decoding step comprises the step of: transforming said ciphertext word signal C] where[by:]

[$M=C^d \pmod{n}$] $M \equiv C^d \pmod{n}$.

[where d is a multiplicative inverse of $e(\text{mod}(\text{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$.]

3. (Twice Amended) A method for [transferring a message signal M_i in a] communications of a message signal M_i cryptographically processed with RSA public key encryption in a system having j terminals, [wherein] each terminal [is] being characterized by an encoding key $E_i = (e_i, n_i)$ and a decoding key $D_i = (d_i, n_i)$, where i=1, 2, . . . , j, and [wherein] the message signal M_i corresponds to a number representative of a message-to-be-received[transmitted] from the i^{th} terminal, the method comprising the steps of:

establishing n_i where n_i is a composite number of the form

[$n_i = P_{i,1} \cdot p_{i,2} \cdot , \ldots , \cdot p_{i,k}$] $n_i = p_{i,1} \cdot p_{i,2} \cdot , \ldots , \cdot p_{i,k}$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to [lcm($p_{i,1}$ -1, $p_{1,2}$ -1, $p_{i,k}$ -1)] lcm($p_{i,1}$ -1, $p_{i,2}$ -1,... $p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1))));[,

comprising the step of:]

receiving by a recipient terminal ($i = y$) from a sender terminal ($i = x$, $x \neq y$) a ciphertext signal C_x formed by encoding a digital message word signal M_x, wherein the encoding includes [M_A for transmission from a first terminal (i=A) to a second terminal (i=B), said encoding step including the sub-step of:]

transforming said message word signal [M_A]M_x to one or more message block word signals [M_A"]M_x", each block word signal [M_A"]M_x" corresponding to a number representative of a portion of said message word signal [M_A]M_x in the range $0 \leq M_x" \leq n_y - 1$ [$0 \leq M_A" \leq n_B - 1$], and

transforming each of said message block word signals [M_A"]M_x" to a ciphertext word signal [C_A, C_A corresponding] C_x that corresponds to a number representative of an encoded form of said message block word signal [M_A"]M_x"[,] where[by:]

[$C_A \equiv M_A"^{eB} \pmod{n_B}$] $C_x \equiv M_x"^{e_y} \pmod{n_y}$; and

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}, p_{y,2}, \ldots, p_{y,k}$ for establishing its d_y.

4. (Twice Amended) A [cryptographic communications] system for communications of a message cryptographically processed with an RSA public key encryption, comprising:

a communication [medium] channel for transmitting a ciphertext word signal C;

[an]encoding means coupled to said channel and adapted for transforming a transmit message word signal M to [a] the ciphertext word signal C using a composite number, n, where n is a product of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

k is an integer greater than 2, and

$p_1, p_2, \ldots p_k$ are distinct random prime numbers [and for transmitting C on said channel],

where the transmit message word signal M corresponds to a number representative of [a] the message and

$0 \leq M \leq n-1$ [where n is a composite number of the form

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and]

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form[and corresponds to]

$C \equiv M^e \pmod{n}$, and

where e is a number relatively prime to lcm(p1 -1, p2 -1, . . . , pk -1); and

[a]decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime numbers $p_1, p_2, \ldots p_k$, for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a [deciphered] decoded form of the ciphertext word signal C [and corresponds to] through a relationship of the form

$M' \equiv C^d \pmod{n}$

where d is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

$e(\text{mod}(\text{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$.

5. (Twice Amended) A [cryptographic communications] system for communications of a message cryptographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, [including] comprising:

a first terminal of the plurality of terminals characterized by an [associated] encoding key

$E_A = (e_A, n_A)$ and a decoding key $D_A = (d_A, n_A)$,

where[in] n_A is a composite number of the form

$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$

where

k is an integer greater than 2,

$p_{A,1}$, $p_{A,2}$, . . . , $p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

lcm($p_{A,1}$ -1, $p_{A,2}$ -1, . . . , $p_{A,k}$ -1), and

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_A (mod(lcm(($p_{A,1}$ -1), ($p_{A,2}$ -1), . . . , ($p_{A,k}$ -1)))); and[,]

[and including]a second terminal of the plurality of terminals having[, comprising:]

blocking means for transforming a first message,[-to-be-transmitted] which is to be transmitted on said communications channel from said second terminal to said first terminal, into one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said first message in the range

$0 \leq M_B \leq n_A - 1$,

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that [and for transmitting C_B on said channel, where C_B] corresponds to a number representative of an [enciphered] encoded form of said first message [and corresponds to] through a relationship of the form

[$C_B \equiv M_B^{eA} \pmod{n_A}$] $C_B \equiv M_B^{e_A} \pmod{n_A}$,

[wherein]said first terminal having [comprises:]

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B from said channel and, having available to it the k distinct random prime numbers $p_{A,1}, p_{A,2}, \ldots, p_{A,k}$, for transforming each of said ciphertext word signals C_B to a receive message word signal [M_B]M'_B, and

means for transforming said receive message word signal[s] [M']M'_B to said first message, where [M']M'_B [is] corresponds to a number representative of a [deciphered] decoded form of C_B [and corresponds to] through a relationship of the form

[$M_B' \equiv C_B^{da} \pmod{n_A}$] $M'_B \equiv C_B^{d_A} \pmod{n_A}$.

6. (Twice Amended) The system according to claim 5 wherein said second terminal is characterized by an [associated] encoding key [E_B =(e_B, n_B)]$\underline{E_B =(e_B, n_B)}$ and a decoding key [DB=(D_B, d_B)]$\underline{D_B =(d_B, n_B)}$, where[:

] n_B is a composite number of the form

$n_B = p_{B,1} \cdot p_{B,2} \cdot \ldots \cdot p_{B,k}$

where k is an integer greater than 2,

$\underline{p_{B,1}, p_{B,2}, \ldots p_{B,k}}$ [$P_{B,1}$, $P_{B,2}$, . . . $P_{B,k}$] are distinct <u>random</u> prime numbers,

e_B is relatively prime to

lcm($p_{B,1}$-1, $p_{B,2}$-1, . . . $p_{B,k}$-1), <u>and</u>

d_B is selected from the group consisting of [the] <u>a</u> class of numbers equivalent to a multiplicative inverse of

e_B (mod(lcm(($p_{B,1}$-1), ($p_{B,2}$ -1), . . . , ($p_{B,k}$ -1)))),

[wherein]said first terminal [comprises:] <u>further having</u>

blocking means for transforming a <u>second</u> message,[-to-be-transmitted] <u>which is to be transmitted on said communications channel</u> from said first terminal to said second terminal, to one or more transmit message word signals M_A, where <u>each</u> M_A corresponds to a number representative of said message in the range

[$0 \leq M_A^{eB} \pmod{n_B}$] $\underline{0 \leq M_A \leq n_B\text{-}1}$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, [

]where C_A corresponds to a number representative of an <u>encoded</u>[enciphered] form of said <u>second</u> message [and corresponds to] <u>through a relationship of the form</u>

[$C_A \equiv M_A^{eB} \pmod{n_B}$] $\underline{C_A \equiv M_A^{e_B} \pmod{n_B}}$

[wherein] said second terminal [comprises;] <u>further having</u>

decoding means coupled to said channel and adapted for receiving <u>each of</u> said ciphertext word signals C_A from said channel and, <u>having available to it the k distinct random prime numbers $p_{B,1}, p_{B,2}, \ldots p_{B,k}$,</u> for transforming each of said ciphertext word signals to a receive message word signal [M_A']$\underline{M'_A}$, and

means for transforming said receive message word signals $[M_A]M'_A$ to said second message, [

]where [M'] M'_A corresponds to a number representative of a [deciphered] decoded form of C_A [and corresponds to] through a relationship of the form

$[M_A' \equiv C_A^{dB} \pmod{n_B}]$ $M'_A \equiv C_A^{d_B} \pmod{n_B}$.

7. (Amended) A method for [establishing cryptographic] communications of a message cryptographically processed with an RSA public key encryption, comprising the steps of:

developing k factors of a composite number n, the k factors being distinct random prime numbers and k is an integer larger than two (k>2);

providing a number e relatively prime to a lowest common multiplier of the k factors;

providing the composite number n;

receiving a ciphertext word signal C which is formed by encoding a digital message word signal M to [a cipher text] the ciphertext word signal C, where said digital message word signal M corresponds to a number representative of [a] said message and

$0 \leq M \leq n-1$,

[where n is a composite number having at least 3 whole number factors greater than one, the factors being distinct prime numbers, and]

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message [word M,] through a relationship of the form

[wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby]

$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$

where e and a_e, a_{e-1}, . . . , a_0 are numbers; and

deciphering the received chiphertext word signal C at an intended recipient with knowledge of the k factors.

8. Cancel claim 8.

9. (Twice Amended) A [communication] system for [transferring] communications of message signals $[M_i]$ cryptographically processed with RSA public key encryption, comprising:

j terminals including first and second terminals[stations], each of the j [stations]terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$[ ], where i=1,2, . . . ,j, [and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,] each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal, and

$0 \leq M_i \leq n_i - 1$,

n_i [is] being a composite number of the form

$[n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}]$ $n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent

to a multiplicative inverse of

$e_i \pmod{\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))}$;

said[a] first terminal [one of the j terminals] including

means for encoding a digital message word signal $[M_A]$ M_1 [for transmission] to be transmitted from said first terminal (i=1[A]) to [a]said second terminal [one of the j terminals] (i=2[B]), said encoding means [for] transforming said digital message word signal $[M_A]M_1$ to a signed message word signal $[M_{As}]$ M_{1s} using a relationship of the form [, M_{1s} corresponding to a number representative of an encoded form of said message word signal M_A,

whereby:]

$[M_{As} \equiv M_A^{dA} \pmod{n_A}]$ $M_{1s} \equiv M_1^{d_1} \pmod{n_1}$; and

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes

means for decoding said signed message word signal M_{1s} to said digital message word signal M_1.

10. (Twice Amended) The system of claim 9, [further comprising:

means for transmitting said signal message word signal M_{As} from said first terminal to said second terminal, and wherein said second terminal includes means for decoding said signed message word signal M_{As} to said digital message word signal M_A, said second terminal including:

means for] wherein the means for decoding said signed message word signal M_{As} includes means for transforming said signed message word signal M_{As}[, whereby] using a relationship of the form

$$[M_A \equiv M_{As}^{e_A} (\mathrm{mod}\, n_A)\,]\; M_1 \equiv M_{1s}^{e_1} (\mathrm{mod}\, n_1).$$

11. (Twice Amended) A communications system for transferring a message signal $[M_i]$ cryptographically processed with RSA public key encryption, the communications system comprising:

j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i=(e_i, n_i)$ and a decoding key $D_i=(d_i, n_i)$, where i=1, 2,. . . , j, [and wherein M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,] each of the j communication stations being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station, and

$0 \le M_i \le n_i - 1$

n_i [is] being a composite number of the form

$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots, p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\mathrm{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots, p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_i \,(\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))))$.

[a] said first station [one of the j communication stations] including

means for encoding a digital message word signal [M_A] M_1 [for transmission] to be transmitted from said first station [one of the j communication stations] (i=1[A]) to [a] said second station [one of the j communication stations] (i=2[B]),

means for transforming said digital message word signal [M_A] M_1 to one or more message block word signals [M_A'] M_1", each block word signal [M_A'] M_1" being a number representative of a portion of said message word signal [M_A']M_1 in the range

$0 \leq M_1'' \leq n_2-1$ [$0 \leq M_A \leq n_B - 1$], and

means for transforming each of said message block word signals [M_A"] M_1" to a ciphertext word signal C_1 using a relationship of the form [C_A, C_A corresponding to a number representative of an encoded form of said message block word signal M_A", whereby:]

[$C_A \equiv M_A''^{Eb} \pmod{n_B}$] $C_1 \equiv M''^{e_2}_1 \pmod{n_2}$; and

means for transmitting said ciphertext word signals C_1 from said first station to said second station, wherein said second station includes

means for deciphering said ciphertext word signals C_1 using $p_{2,1}, p_{2,2}, \ldots, p_{2,k}$ to produce said message word signal M_1.

12. (Twice Amended) The communications system of claim 11,[further comprising:

means for transmitting said ciphertext word signals from said first terminal to said second, and]

wherein [said second terminal] the deciphering means includes

means for decoding said ciphertext word signals C_1 to said message block word signals [MA] M_1" using a relationship of the form[, said second terminal including:

means for transforming each of said ciphertext word signals C_A to one of said message block word signals M_A", whereby

$M_A'' \equiv C_A^{Db} \pmod{n_B}$] $M''_1 \equiv C_1^{d_2} \pmod{n_2}$, and

means for transforming said message block word signals [M_A"] M_1" to said message word signal [M_A]M_1.

13. (Twice Amended) [In a] A [communications] system for communications of a message cryptographically processed with RSA public key encryption, [including] comprising:

a first station; and

[and] a second [communicating] station[s inter] communicatively connected to the first station [for communication therebetween],

the first [communicating] station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where the transmit message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n-1$

[where] n [is] being a composite number formed as a product of [having] at least 3 [whole number] factors [greater than one], the at least 3 factors being distinct random prime numbers, and

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form [and corresponds to]

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and a_e, a_{e-1}[-1], . . . , a_0 are numbers; and

means for transmitting the ciphertext word signal C to the second [communicating] station, wherein the second station includes means for deciphering the chipertext word signal C using the at least 3 factors to produce the message.

New Claims:

14. (Amended) A method of communicating a message cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion *e* associated with a recipient intended for receiving the message;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message formed by encoding a plaintext message data *M* to the ciphertext message data *C* using a relationship of the form $C \equiv M^e \pmod{n}$, where *M* represents the message, where $0 \leq M \leq n-1$ and where the sender knows n and the public key portion e but has no access to the *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$; and

deciphering at the recipient the received ciphertext message data *C* to produce the message, the recipient having access to the *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$.

15. (Amended) The method according to claim 14, comprising the further step of:

establishing a private key portion *d* by a relationship to the public key portion *e* in the form of

$$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1))),$$

wherein the deciphering step includes decoding the ciphertext message data *C* to the plaintext message data *M* using a relationship of the form $M \equiv C^d \pmod{n}$.

16. (Amended) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion *e*;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1} (\text{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)));$$

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message data C representing an encoded form of a plaintext message data M; and

decoding the received ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$, the decoding performed by a recipient owning the private key portion d and having access to the k distinct random prime numbers, p_1, $p_2, \ldots p_k$.

17. (Amended) The method according to claim 16, wherein the ciphertext message data C is formed by encoding the plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no access to the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

18. (Amended) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e of the form

$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

computing a composite number, n, as a product of the *k* distinct random prime numbers;

encoding a plaintext message data *M* with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$

receiving the signed message M_s; and

deciphering the signed message to produce the plaintext message data *M*.

19. (Amended) The method of claim 18, wherein the deciphering step includes:

decoding the signed message M_s with the public key portion e to produce the plaintext message data *M* using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. (Amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

sending to a recipient a cryptographically processed message formed by

assiging a number *M* to represent the message in plaintext message form, and

cryptographically transforming the assigned number *M* from the plaintext message form to a number *C* that represents the message in an encoded form, wherein the number *C* is a function of

the assigned number *M*,

a number *n* that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent *e* that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number *n* and exponent *e* having been obtained by the sender are associated with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based on

the number *n*,

another exponent *d*, and

the number *C*,

wherein the exponent *d* is a function of the exponent *e* and the at least three distinct random prime numbers.

21. (Amended) The method according to claim 20,

wherein the cryptographically transforming step includes using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent *d* is established based on the at least three distinct random prime numbers, $p_1, p_2, \ldots p_k$, using a relationship of the form $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$, and

wherein the cryptographically processed message is deciphered using a relationship of the form $M \equiv C^d \pmod{n}$.

22. (Amended) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

receiving from a sender a cryptographically processed message, in the form of a number *C*, which is decipherable by the recipient based on a number *n*, an exponent *d*, and the number *C*; and

deciphering the cryptographically processed message,

wherein a number *M* represents a plaintext form of the message, wherein the number *C* represents a cryptographically encoded form of the message and is a function of the number *M*,

the number *n* that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent *e* that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number *n* and exponent *e* are associated with the recipient to which the message is intended, and

wherein the exponent *d* is a function of the exponent *e* and the at least three distinct random prime numbers.

23. (Amended) The method according to claim 22,

wherein the number *C* is formed using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent *d* is established based on the at least three distinct random prime numbers, $p_1, p_2, \ldots p_k$, using a relationship of the form $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$,

and wherein the number *M* is obtained using a relationship of the form $M \equiv C^d \pmod{n}$.

24. (Amended) The method according to claim 21,

wherein *p* and *q* are a pair of prime numbers the product of which equals *n*,

wherein the deciphering the number *C* to derive the number *M* is divided into subtasks, one subtask for each of the *k* distinct random prime numbers,

wherein the *k* distinct random prime numbers are each smaller than *p* and *q*,

whereby for a given length of *n* it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers *p* and *q* were used instead.

25. (Amended) The method according to claim 22,

wherein *p* and *q* are a pair of prime numbers the product of which equals *n*,

wherein the deciphering the number *C* to derive the number *M* is divided into subtasks, one subtask for each of the *k* distinct random prime numbers,

wherein the *k* distinct random prime numbers are each smaller than *p* and *q*,

whereby for a given length of *n* it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers *p* and *q* were used instead.

26. (Amended) The method according to claim 20,

wherein *p* and *q* are a pair of prime numbers the product of which equals *n*, and

wherein developing the at least three distinct random prime numbers and computing *n* is performed, including for *n* that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers *p* and *q* and compute that *n*.

27. (Amended) The method according to claim 22,
wherein *p* and *q* are a pair of prime numbers the product of which equals *n*, and
wherein developing the at least three distinct random prime numbers and computing *n* is performed, including for *n* that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers *p* and *q* and compute that *n*.

28. (Amended) The method according to claim 14,
wherein *p* and *q* are a pair of prime numbers the product of which equals *n*,
wherein the deciphering step is divided into sub-steps, one sub-step for each of the *k* distinct random prime numbers,
wherein the *k* distinct random prime numbers are each smaller than *p* and *q*,
whereby for a given length of *n* it takes fewer computational cycles to perform the deciphering step relative to the number of computational cycles for performing such deciphering step if the pair of prime numbers *p* and *q* were used instead.

29. (Amended) The method according to claim 14,
wherein *p* and *q* are a pair of prime numbers the product of which equals *n*, and
wherein developing the *k* distinct random prime numbers and computing the composite number *n* are performed, including for *n* that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers *p* and *q* and compute that *n*.

30. (Amended) The method according to claim 16,
wherein *p* and *q* are a pair of prime numbers the product of which equals *n*,
wherein the decoding step is divided into sub-steps, one sub-step for each of the *k* distinct random prime numbers,
wherein the *k* distinct random prime numbers are each smaller than *p* and *q*,

whereby for a given length of n it takes fewer computational cycles to perform the decoding step relative to the number of computational cycles for performing such decoding step if the pair of prime numbers p and q were used instead.

31. (Amended) The method according to claim 16,
wherein p and q are a pair of prime numbers the product of which equals n, and
wherein developing the k distinct random prime numbers and computing the composite n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

32. (Amended) The method according to claim 18,
wherein p and q are a pair of prime numbers the product of which equals n,
wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,
wherein the k distinct random prime numbers are each smaller than p and q,
whereby for a given length of n it takes fewer computational cycles to perform the encoding step relative to the number of computational cycles for performing such encoding step if the pair of prime numbers p and q were used instead.

33. (Amended) The method according to claim 18,
wherein p and q are a pair of prime numbers the product of which equals n, and
wherein developing the k distinct random prime numbers and computing the composite number n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

34. (Amended) The method according to claim 14, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable with multi-prime ($k>2$) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, $p_1, p_2, \ldots p_k$.

35. (Amended) The method according to claim 9, wherein the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed at the first terminal with multi-prime ($k>2$) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, . . . pk, is decipherable at the second terminal with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

36. (Amended) The method according to claim 16, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable by the decoding with multi-prime ($k>2$) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, . . . p_k.

37. (Amended) The method according to claim 18, wherein the signed message M_s, formed from the plaintext message data M being cryptographically processed at the sender with multi-prime ($k>2$) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, . . . pk, is decipherable by the decoding at the recipient with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q. .

38. (Amended) The method according to claim 20, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (Amended) The method according to claim 22, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being

equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (Amended) A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)));$$

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n; and

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n$-1, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n.

41. The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. (Amended) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to communicate with the plurality of stations via the communications medium sending a receiving messages cryptographically processed with an RSA public key encryption, the host system including

at least one cryptosystem configured for

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

in response to an encoding request from the host system, encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

in response to a decoding request from the host system, decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^{d} \pmod{n}$.

43. (Amended) A system for communications of a message cyptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem communicatively coupled to and receiving from the bus encoding and decoding requests, the cryptosystem being configured for

providing a public key portion e,

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C, a ciphertext form of the first message, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, and

in response to an decoding request from the host system, decoding C', a ciphertext form of a second message, to produce M', a plaintext form of the second message, using a relationship of the form $M' \equiv C'^d \pmod{n}$, the first and second messages being distinct or one and the same.

44. The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (Amended) The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory coupled to the processor via the data-address bus,

a data encryption standard (DES) unit coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (Amended) The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that cryptographically processes message data received/returned from/to the processor.

47. (Amended) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit is configured to recognize the secure and exponentiator elements address spaces and to automatically encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the processor is

accessing the insecure memory address spaces, the DES unit being further configured to decode encoded message data received from the memory before it is provided to the processor.

48. The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding request providing a plaintext message M to be encoded,

obtaining a public key that includes an exponent e and a modulus n, a representation of the modulus n existing in the memory in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$,

constructing subtasks, one subtask for each of the k factors, to be executed by the exponentiator elements for producing respective ones of the subtask values, $C_1, C_2, \ldots C_k$, and

forming a ciphertext message C from the subtask values $C_1, C_2, \ldots C_k$,

wherein the ciphertext message C is decipherable using a private key that includes the modulus n and an exponent d which is a function of e.

51. (Amended) The system of claim 50 wherein each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $M_i \equiv M (\text{mod } p_i)$, and $e_i \equiv e (\text{mod } p_i - 1)$, and where i=1, 2, ... *k*.

52. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding/decoding request provided with a plaintext/ciphertext message *M/C* to be encoded/decoded and with or without a public/private key that includes an exponent *e/d* and a modulus *n* a representation of which exists in the memory in the form of its *k* distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$,

obtaining the public/private key from the memory if the encoding/decoding request is provided without the public/private key,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \ldots M_k / C_1, C_2, \ldots C_k$, and

forming the ciphertext/plaintext message *C/M* from the subtask values $C_1, C_2, \ldots C_k / M_1, M_2, \ldots M_k$.

53. (Amended) The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\text{mod } p_i)$, where $C_i \equiv C (\text{mod } p_i)$, and $e_i \equiv e (\text{mod } p_i - 1)$, and where i=1, 2, ... *k*.

54. (Amended) The system of claim 52 wherein when produced each one of the subtasks M_1, M_2, . . . M_k is developed using a relationship of the form $M_i \equiv C_i^{d_i} (\mathrm{mod}\, p_i)$, where $M_i \equiv M (\mathrm{mod}\, p_i)$, and $d_i \equiv d (\mathrm{mod}\, p_i - 1)$, and where i=1, 2, ... k.

55. The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$.

56. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, p_1, p_2, . . . p_k, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for receiving a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d (\mathrm{mod}\, n)$.

57. The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e (\mathrm{mod}\, n)$, where $0 \leq M \leq n$-1.

58. (Amended) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers; and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$, the signed message M_s being decipherable using the public key portion e.

59. (Amended) The system of claim 58 further comprising the step of:

means for decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. (Amended) The system of claim 57, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (Amended) The system of claim 59, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.